



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,960	09/03/2004	Alexander Shipp	117-516	1450
23117	7590	10/10/2007		
NIXON & VANDERHYE, PC 901 NORTH GLEBE ROAD, 11TH FLOOR ARLINGTON, VA 22203				
			EXAMINER NALVEN, ANDREW L	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 10/10/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/500,960	<b>Applicant(s)</b> SHIPP, ALEXANDER	
	<b>Examiner</b> Andrew L. Nalven	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 08 July 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 6-10 is/are rejected.
- 7) ☒ Claim(s) 5 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 July 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>9/3/2004, 7/8/2004</u> . | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

1. Claims 1-10 are pending.

### ***Specification***

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

#### **Arrangement of the Specification**

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
- (e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
- (f) BACKGROUND OF THE INVENTION.
  - (1) Field of the Invention.
  - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (g) BRIEF SUMMARY OF THE INVENTION.
- (h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (i) DETAILED DESCRIPTION OF THE INVENTION.
- (j) CLAIM OR CLAIMS (commencing on a separate sheet).
- (k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

***Claim Objections***

2. Claim 2 is objected to because of the following informalities:
  - a. The word "categorised" should be corrected to read, "categorized."
  - b. The word "signalling" should be corrected to read, "signaling."
3. Claim 4 is objected to because of the following informalities:
  - c. The word "signalling" should be corrected to read, "signaling."
4. Claim 6 is objected to because of the following informalities:
  - d. The word "signalling" should be corrected to read, "signaling."
5. Claim 7 is objected to because of the following informalities:
  - e. The word "categorised" should be corrected to read "categorized."
  - f. The word "signalling" should be corrected to read, "signaling."
6. Claim 9 is objected to because of the following informalities:
  - g. The word "signalling" should be corrected to read, "signaling."
7. Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. **Claims 1-4 and 6-9 are rejected under 35 U.S.C. 102(e)** as being anticipated by Stolfo et al US PGPub 2003/0167402.

9. **With regards to claim 1**, Stolfo teaches a method of anti-virus processing an email having an executable attachment comprising the steps, executed by a machine (Stolfo, paragraph 0045, mail server extracts attachments and analyzes attachments for malicious code), of: a) extracting structural elements from the email (Stolfo, paragraph 0044, mail is logged noting the set of properties for that email); b) examining the executable attachments for code, data or encoded data that could have created the structural elements extracted earlier (Stolfo, paragraph 0061, data analysis component examines records about attachments to determine if malicious); and c) signalling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails

is too high, paragraph 0046, looks at portions of email that are replicated without change).

10. **With regards to claim 2**, Stolfo teaches the structural elements are categorized and the step c) includes assigning a numeric score for each element which could have been created by that attachment, and signaling that the attachment is possibly viral or not on the basis of an overall score (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0051, statistical model relating to attachment behavior, paragraph 0057, notes reference code, sender, receiver, number of recipients).

11. **With regards to claim 3**, Stolfo teaches that the scores are weighted according to category (Stolfo, paragraphs 0059-0061, probabilistic model generates numerical figure from analysis of data records).

12. **With regards to claim 4**, Stolfo teaches signaling step c) takes account of factors including any or all of the following attributes of the email: standard MIME headers; unusual MIME headers; deviations from RFC standards; unusual constructs; number of attachments; type of attachments; encoding method used for attachments; text content of the email; and HTML or XHTML content of the email (Stolfo, paragraph 0057, notes reference code, sender, receiver, number of recipients, paragraph 0054, birth rate of new emails with the attachment).

13. **With regards to claim 6**, Stolfo teaches a system for anti-virus processing an email having an executable attachment comprising the following means, implemented by a machine (Stolfo, paragraph 0045, mail server extracts attachments and analyzes

Art Unit: 2134

attachments for malicious code): a) means for extracting structural elements from the email (Stolfo, paragraph 0044, mail is logged noting the set of properties for that email); b) means for examining the executable attachments for code, data or encoded data that could have created the structural elements extracted earlier (Stolfo, paragraph 0061, data analysis component examines records about attachments to determine if malicious); and c) means for signaling that the attachment is possibly viral or not on the basis of the extent to which the examining step b) finds evidence that the structural elements have been created by that attachment (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0046, looks at portions of email that are replicated without change).

14. **With regards to claim 7**, Stolfo teaches the structural elements are categorized and the means c) includes means for assigning a numeric score for each element which could have been created by that attachment, and signaling that the attachment is possibly viral or not on the basis of an overall score (Stolfo, paragraph 0054, attachment is malicious if birth rate of new emails is too high, paragraph 0051, statistical model relating to attachment behavior, paragraph 0057, notes reference code, sender, receiver, number of recipients).

15. **With regards to claim 8**, Stolfo teaches the scores are weighted according to category (Stolfo, paragraphs 0059-0061, probabilistic model generates numerical figure from analysis of data records).

16. **With regards to claim 9**, Stolfo teaches the signalling step c) takes account of factors including any or all of the following attributes of the email: standard MIME

Art Unit: 2134

headers; unusual MIME headers; deviations from RFC standards; unusual constructs; number of attachments; type of attachments; encoding method used for attachments; text content of the email; and HTML or XHTML content of the email (Stolfo, paragraph 0057, notes reference code, sender, receiver, number of recipients, paragraph 0054, birth rate of new emails with the attachment).

### ***Allowable Subject Matter***

Claims 5 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

17. The following is a statement of reasons for the indication of allowable subject matter: The cited prior art, Stolfo and Schultz, teach methods of detecting viruses in emails. However, the cited prior art fails to specifically teach a means for extracting the structural elements as strings and examining the attachments for matches of those strings and signaling the attachment as possibly viral or not on the basis of the extent to which the examining finds occurrences of the strings in the attachment. Thus, the cited prior art fails to anticipate or render obvious the above-cited claims.

### ***Conclusion***



Art Unit: 2134

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Schultz et al US PGPub 2003/0065926 discloses a method for detecting of new malicious executables.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

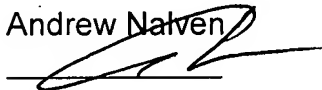
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/500,960

Page 9

Art Unit: 2134

Andrew Nalven

A handwritten signature in black ink, appearing to read 'Andrew Nalven', written over a horizontal line.